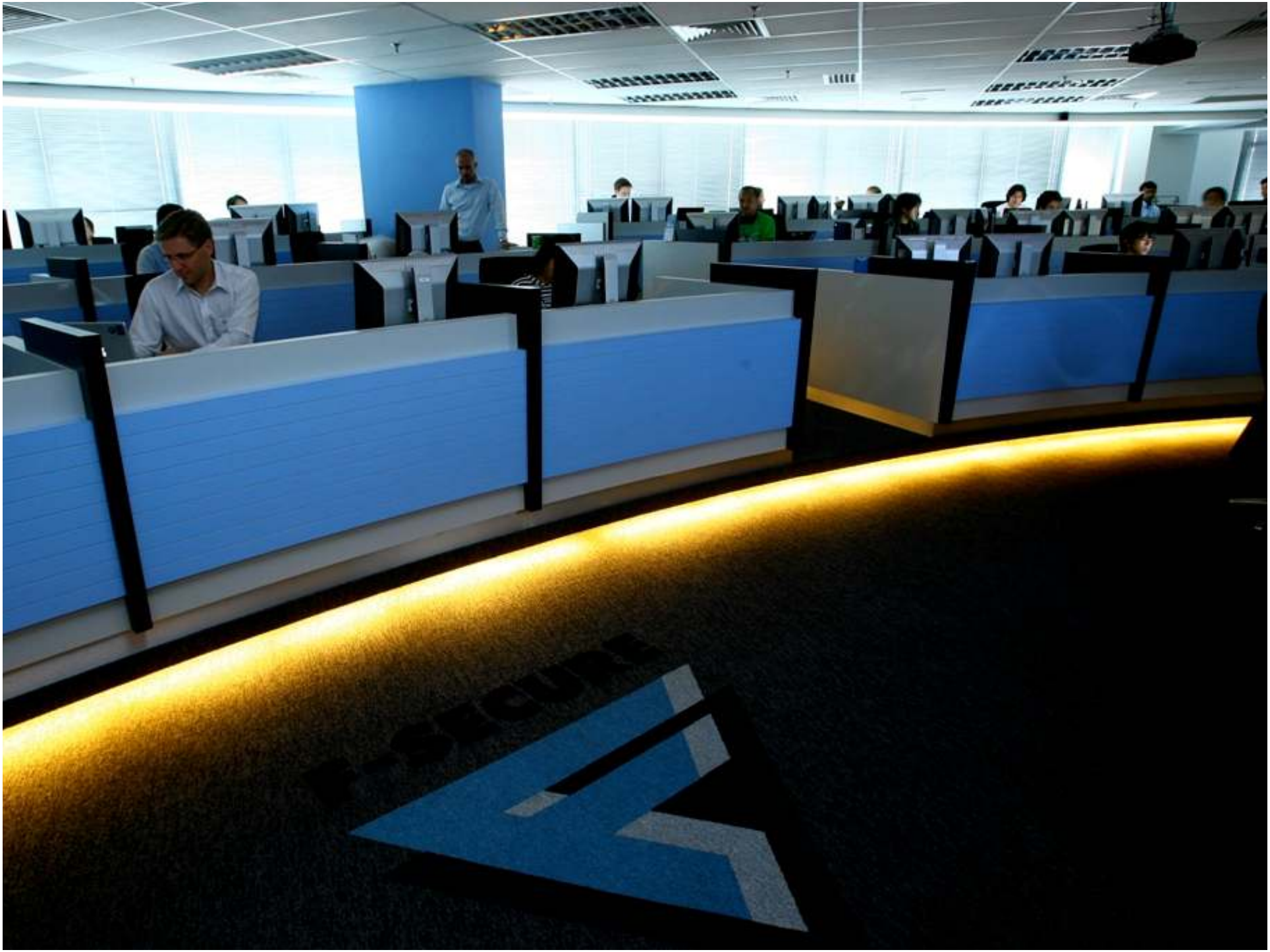
# Current Mobile Phone Threats

Jarno Niemelä
F-SECURE®

BE SURE.


F-SECURE

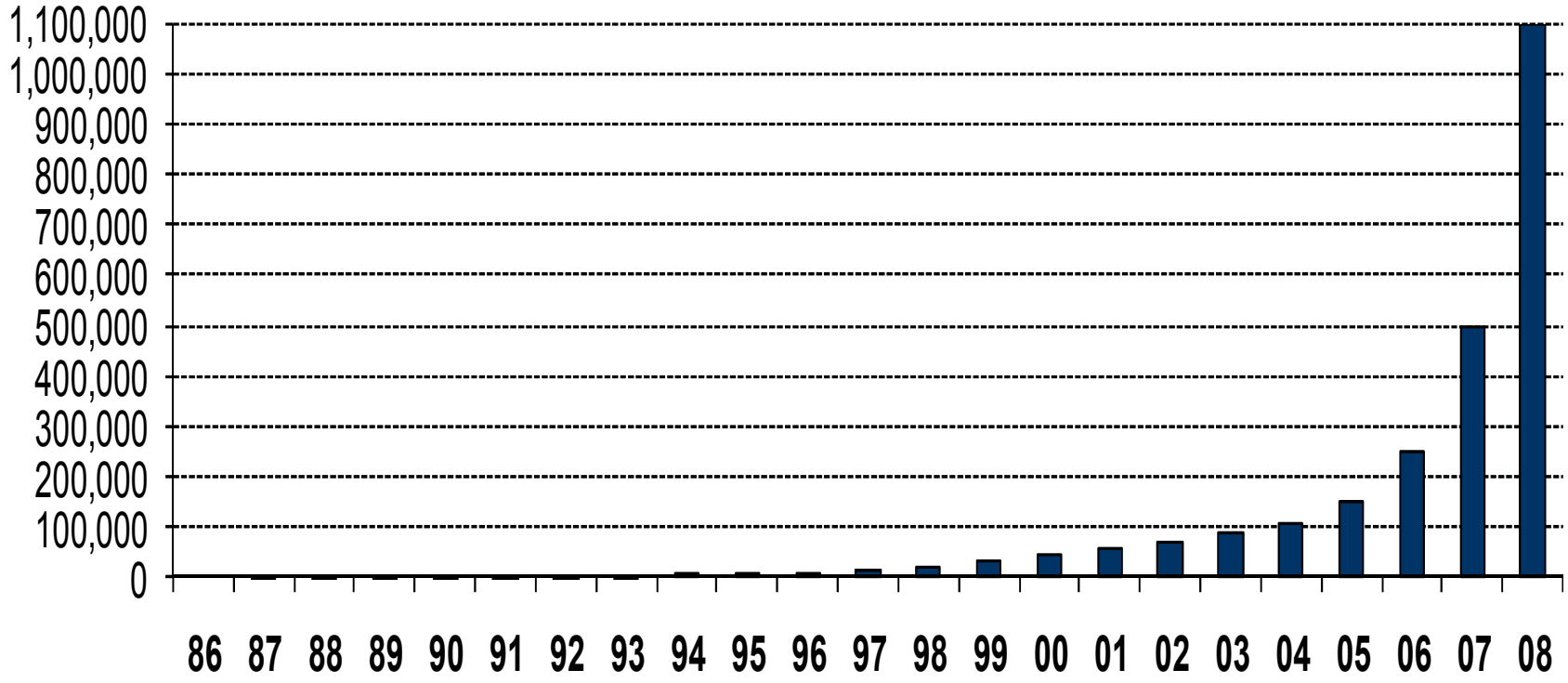



F-SECURE®

BE SURE.

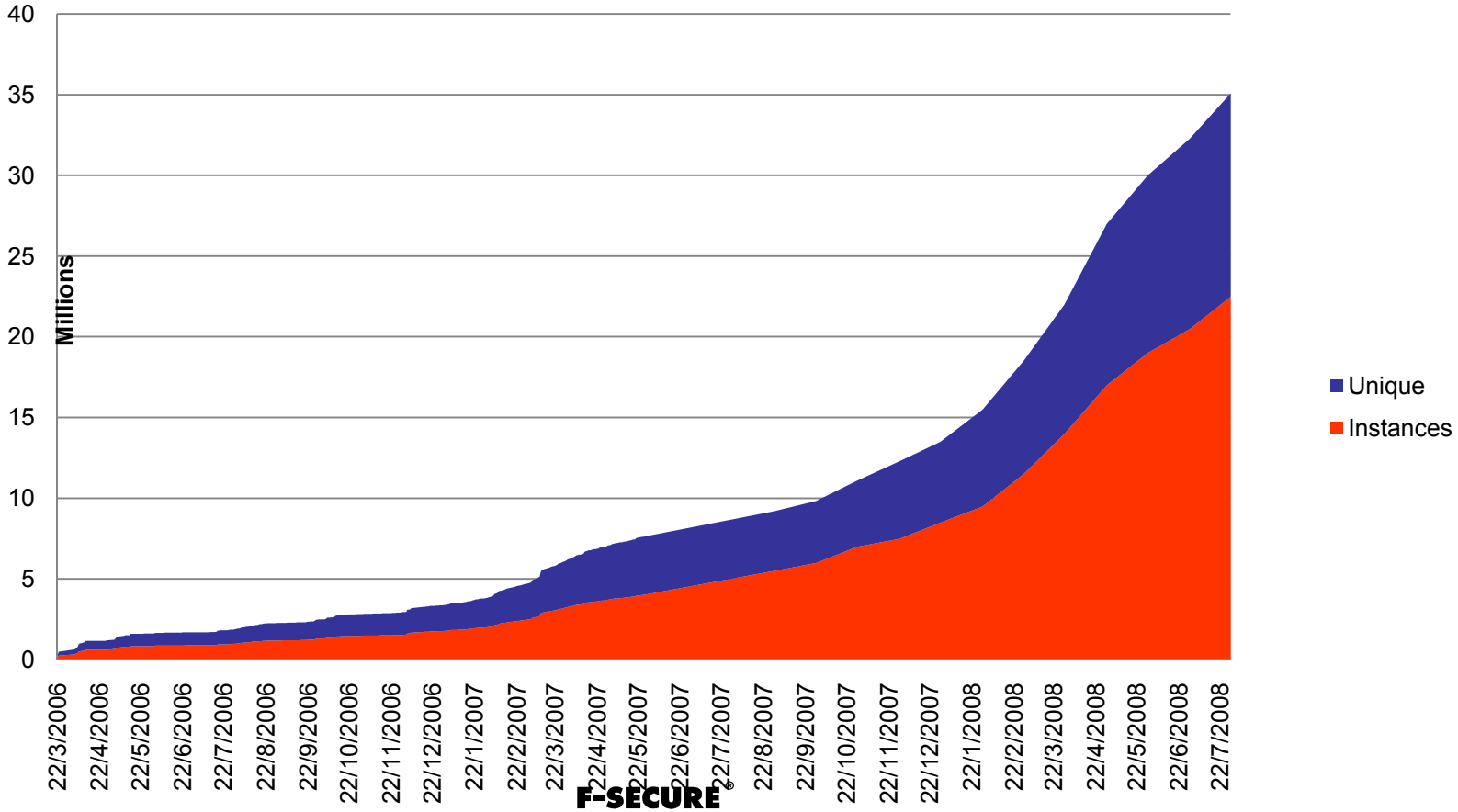

So, where are we now?

# Number of virus detections in F-Secure products




F-SECURE®
BE SURE.

# Malware samples in F-Secure's collection




F-SECURE®

BE SURE.

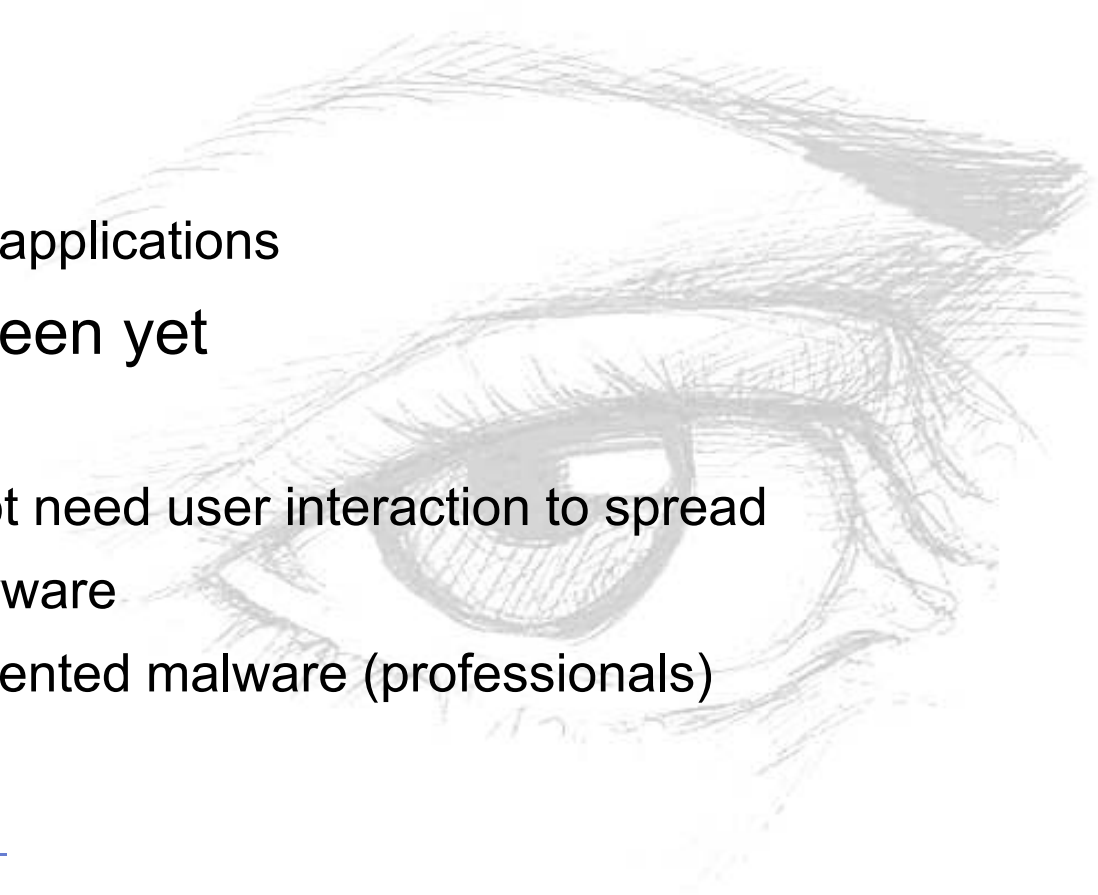
# Types of Mobile Threats

What we have seen so far

- Viruses
- Worms
- Trojans
- Single target spying applications

What we have not seen yet

- Rootkits
- A worm that does not need user interaction to spread
- Mass distributed spyware
- Large scale profit oriented malware (professionals)



# Viruses And Worms

Viruses and Worms spread over

- Bluetooth file transfers
- MMS messages
- Infected memory cards

When a new worm appears it causes an initial outbreak

- Typically the initial outbreak is over MMS, which continues until operator starts to filter the messages
- After initial outbreak the continues to spread in the background over Bluetooth and memory card transfers
- As most of users who can get infected do not have on device anti-virus, viruses and worms basically never go away

# Case SymbOS/HatiHati

Symbian anti-theft software that turned into disaster

- HatiHati is 0.95 version of Guardian Symbian anti-theft tool

Guardian is supposed to

- Detect if SIM card is changed in the phone
- Lock the phone
- Send SMS message with information of new SIM card
- Survive phone reformat by hiding in MMC card and reinstalling itself in to phone after format

Current versions do the above, and Guardian is widely used

# However version 0.95 had some bugs

Instead sending message only once 0.95 goes into infinite loop

- The infected phone is sending messages as fast as it can
- Which means in average once per 7 seconds or so
- Even with small population you can get 100000s SMS per hour

Also the format survival had a small bug

- Guardian starts automatically from memory card at phone boot or memory card insert
- 0.95 does not check if the phone where it is inserted the one that it is supposed to protect
- Which means that any phone where infected MMC is inserted gets infected and starts sending SMS messages

# Trojans

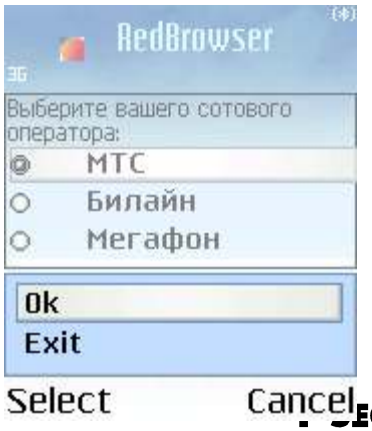
Trojans are stand alone malware that do no spread by itself

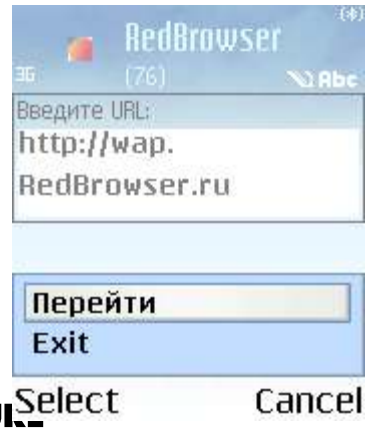
- Trojans are Symbian or Windows mobile installation packages that pretend to be beneficial applications
- When a trojan is installed it tries to harm the device in some way, either by destroying data or blocking phone functionality
- In addition of just breaking the phone, trojans almost always carry viruses or worms that they infect the device it as additional nuisance
- Trojans are mostly distributed over various file sharing groups
- Trojan creator or someone else uploads the trojan into forum with misleading name or description as a joke

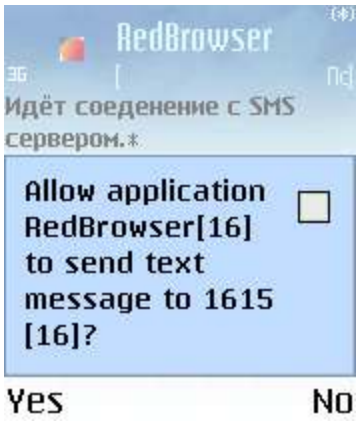
# Making Money With Trojans

Some trojans send SMS messages to premium rate numbers

- When the trojan application is executed it shows some social engineering text and either sends SMS messages directly or asks for user permission
- So far we have not been able to determine whether any profit is being made this way, or are the premium rate numbers chosen at random

# SMS Spam And Phishing

SMS spam and phishing have been with us quite a while

- Now and then we get reports of mobile users being spammed with SMS that contains some kind of phishing scheme
- Usually the goal is to get people to call some premium rate number, or fool them to get subscribed to some expensive content service
- We have also seen messages that pretend to be from a bank or credit service, and if victim calls to number in SMS they get connected to fraudster that tries to get their banking details or fool them in some other way.
- All in all same kind of financial scams that have existed long before mobiles are now trying to make initial contact over SMS

# Case HelloCarbide

**HelloCarbide is standalone Symbian jailbreak**

- HC uses the same AppTrk vulnerability that has been already been used to disable Symbian platform security
- The previous attack was cumbersome as it required PC, USB and lot of manual steps
- HC eased things by packing the jailbreak code into single application that installs nicely as SIS package
- HC disables capabilities checking from any process that is currently running
- Which means that if you have file manager open before starting HC, you can access sys\bin or any other place that is normally forbidden
- The downside is that after HC you cannot launch applications

# What HelloCarbide Means For Security

**HelloCarbide and ROMPatcher have UI so they are not directly usable for malware**

- But anyone with IDA, time and skill can reverse engineer HC and ROMPatcher and include that into installation of his malware
- Which means that pretty soon we will see Commwarrior or Beselo for S60 3rd edition
- Lets hope we get it only after vacations

# Mobile Spy Tools

Mobile spy tools are applications that are installed onto a phone to send information out from the phone

- Typical example - an application that forwards all received SMS messages to a third party without the user's permission

Mobile spy tools are not illegal in and of themselves

- Their vendors state (weakly in most cases) that they must only be used for legal purposes
- While in reality most of the things for which people use these tools are illegal; or at least they are in countries that have strong privacy protection laws

# Who Would Use Spy Tools

The same people who use PC based spy tools

- Oppressive spouses and other domestic abuse cases
- Private investigators / divorce attorneys
- Managers monitoring their employees
- Industrial spies

Some vendors sell both PC and mobile spy tools

- And give discounts if you buy both
- Spy both on your wife's PC and her mobile phone

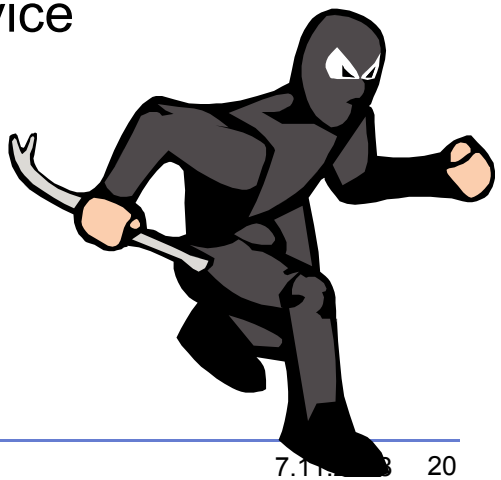
# Targeted and Untargeted Spy Tools

Targeted spy tools are limited by the vendor

- A spy must know the victim before obtaining the spy tool
- Limitations are usually applied by requiring the target device's IMEI code in order to obtain the spy software
- So the spy needs to have access to the device at least twice
- This is done by spy tool authors more as copy protection than concern on how their software is going to be used

Untargeted spyware can be installed onto any device

- The victim of the spy tool can be picked at random
- The spy needs to access the device only once



# Information That Can Be Stolen

SMS and MMS traffic information and content

- Sender and receiver phone numbers and phone book names
- The content of the SMS or MMS message

E-Mail traffic information and content

- Sender and receiver addresses
- E-mail text and attachments

SIM card information

- Sends the SIM IMSI and phone number as soon as new SIM is inserted

F-SECURE®

BE SURE.

# Information That Can Be Stolen

## Call information

- Incoming or outgoing call and to what number
- Time and duration of the call

## Voice recording

- Application can record all phone calls to memory card
- The attacker either needs to access the card to get the recordings or they are sent over Bluetooth, MMS, or HTTP

## Call interception

- Allows for tapping into voice conversations by setting a covert conference call

# Information That Can Be Stolen

## Remote listening

- When a specific number calls, the phone will answer silently
- The phone will not give any indication that a call is open
- Some spyware will even allow automatic conference calls

## Physical location

- Some tools are capable of using built-in GPS in modern phones, and to send GPS coordinates
- Those that don't use GPS send GSM cell ID and signal info

## User key presses

- All user key presses can be logged and sent over SMS

# Typical Spy Tool Operation

## Installation

- Spy applications are installed using the normal application install like any other application
- Although most of them fail to mention what the application is

## Hiding

- When the spy application has activated it will hide itself
- The application will not be visible in application task list
- It will not be visible in user interface or application manager
- All log information of sent SMS messages or data connections will be erased as soon as the spy messages have been sent

# Typical Spy Tool Operation

## Information gathering

- Spy tool hooks all messaging APIs in which it is interested
- Or it simply reads the content from application data files

## Leaking user personal data back to attacker

- Spy tool sends the information either in SMS messages or connects to a remote server and sends data over TCP/IP
- Some tools send data instantly after user event and others use timed delay or a certain number of messages in order to minimize number of transmissions

# Methods of Selling Spy Tools

## Web shops

- Licences and software sold on typical E-store
- Software is either IMEI locked or uses server to store info
- Payment over credit card, Paypal, E-gold, etc

## Spy shops

- Most spying equipment shops also sell software or phone modification services

## OEM spy tools

- Some spy tool manufacturers sell easy to use spy tool generators for spy shops

# Devices affected by spyware

Software

•Symbian OS 6.x-8x

- 6670, 6630, N70,6680,9210,etc

•Symbian S60 3rd edition

- E60,E61,E50,E70,E90,etc

Windows mobile

- 2003, 2003 SE, 5.0 and 6.0

LG

- LG JOY

•Sony Ericsson UIQ devices

- P800, P900, M600, W950

Hardware

•Flash OS “upgade”

- Nokia 1100, 3120,3310

•Modifications on actual harware

- Remote listening is available for most phone models

# FlexiSpy

FlexiSpy.A was invasive enough to be classified as a trojan
Later variants are classified as riskware

FlexiSpy monitors

- Voice call destinations
- Voice call times dates and duration
- SMS messaging and contents

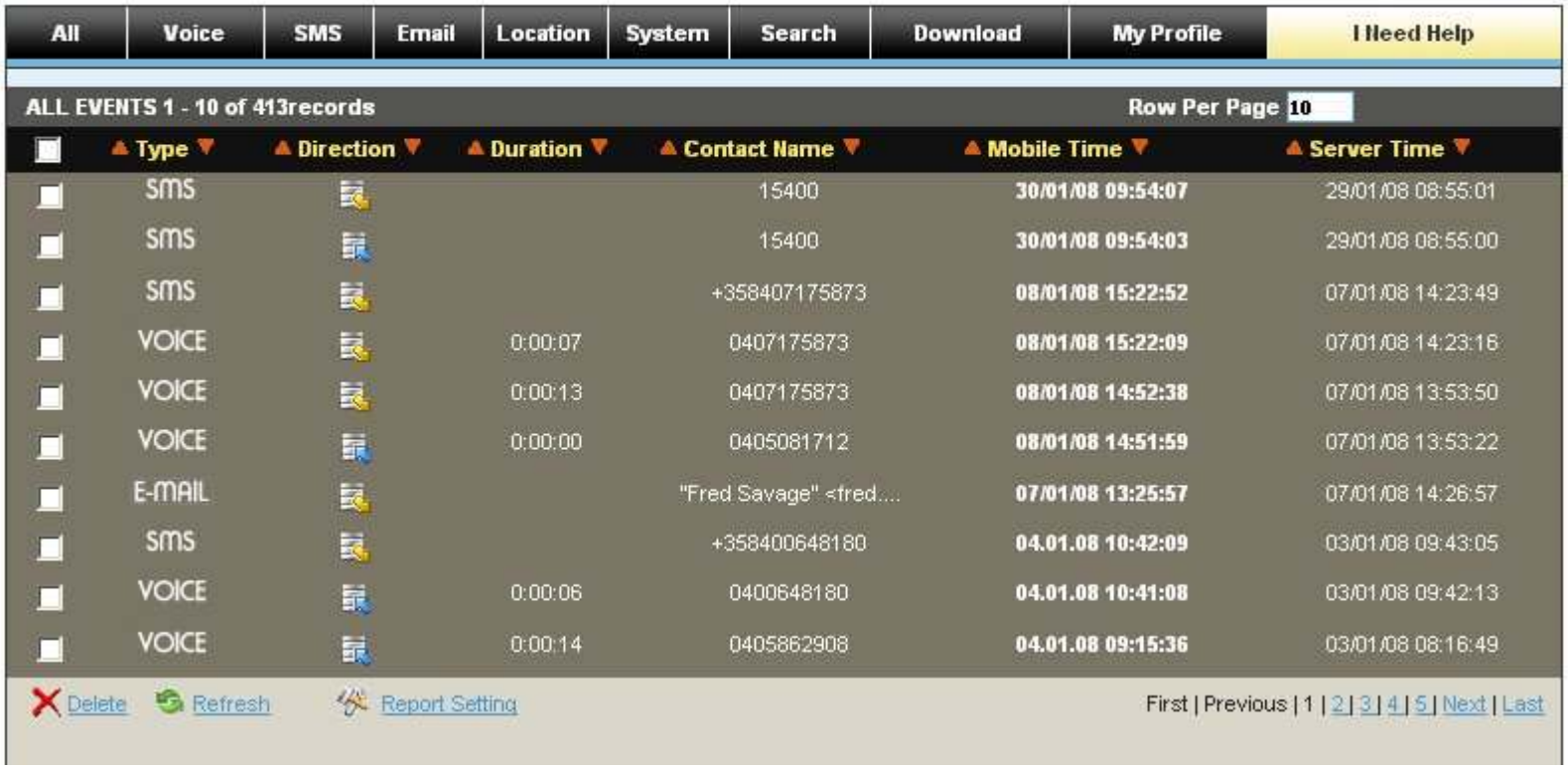
Software itself is not illegal

- Unauthorized installation of it is



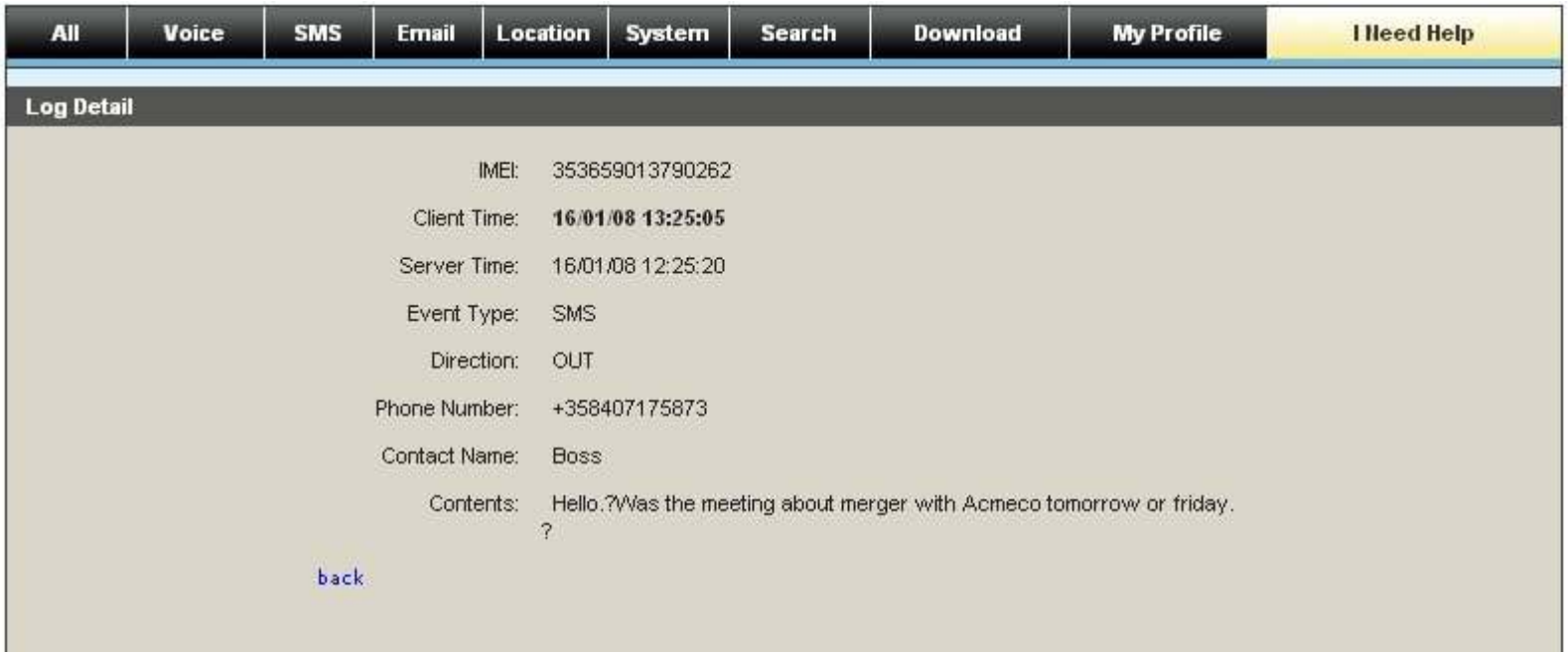
F-SECURE®
BE SURE.

# FlexiSpy web interface




F-SECURE®
BE SURE.

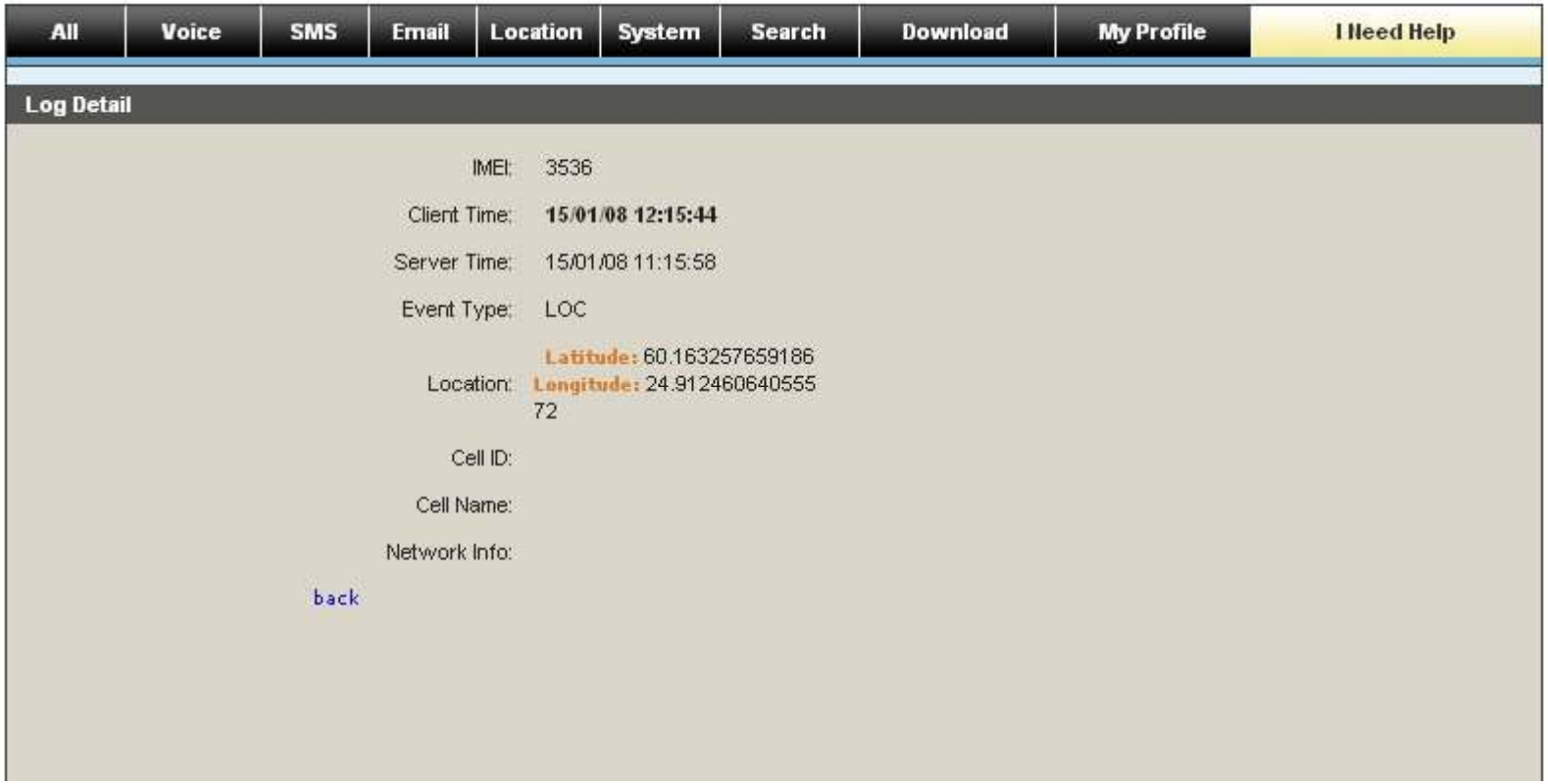
# SMS Messages




F-SECURE®
BE SURE.

# Voice Call Information

# GPS Location Information



' or "hotels near lax"

0640555 Search Maps

d businesses Get directions

# FlexiSpy on Symbian S60 3rd Edition

**The latest versions also work on S60 3rd edition phones**

- Nokia E60, E61, E65, E70, E95, N73, N95 and all other new models
- The software is **Symbian Signed**, so it passes all security checks

**So how did spy tool pass Symbian Signed?**

- By using social engineering
- Software was submitted as a fictional application **"RBackupPRO"**
- "RBackupPRO" was described as a remote backup software that copies user data to a remote server. And thus needs access to user data and network.
- So when the application was approved, everything was working as documented!

# The Other Side of the Coin

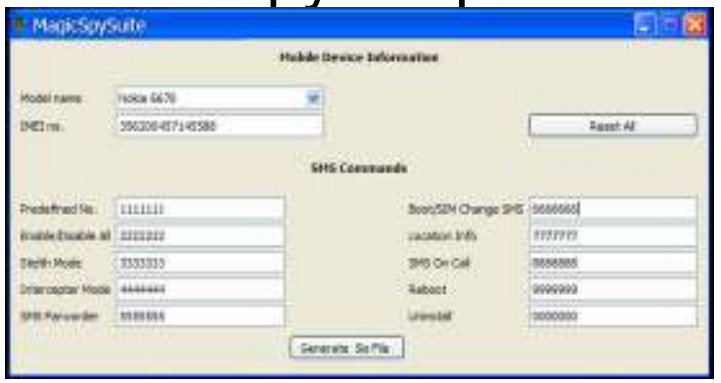
When Flexispy is installed spying features are disabled

- The attacker must enter a secret code to access the hidden user interface
- From this interface the software is activated and spying features are enabled
- Thus a remote backup tool is suddenly a very capable spy tool

Symbian has no resources for exhaustive checks

- Thus any other application with hidden functionality can pass the checks with high probability of success


# Magic Spy suite is a spy tool generator for spy shops




- Anyone can buy the generator and set up their own spy shop
- We have seen similar tools for PCs
- But this is first for mobile devices
- It's a good bet that many of the spy shops that can be found with Google actually use this tool
- Current license price 12,500 $US

# Detecting Spy Tools

Spy tools are problematic to detect

- Spy tool vendors have an interest in staying below the radar of security companies
- Which means that AV companies do not have full sample set, and therefore we do not have near full detection coverage like we have with other threats

F-Secure Anti-Virus detects everything we have seen

- But let's have a look at tools and methods to handle cases that we have not yet seen

# Best Defence, Be Prepared

You need to know what clean system looks like

- Take file system copy from each phone model that is given to users
- Get a list of processes that are running on default user configuration
- Make sure you have necessary tools to investigate the phone
- If your company does regular bug sweeps, do make sure that phone check is in the process

# Preventing Spy Tools on Phones

Use Anti-Virus

- Good AV detects the most commonly used spy tools

All phones must have up to date OS

- Some installation methods rely on OS bugs

Every phone must have lock code

- While phone is locked no new applications can be installed

Have users personalize their phones

- Prevents quick swapping of the phone

Configure the phone to allow only signed applications

# Preventing Spy Tools on Phones

Have the phone OS of key personal flashed at regular intervals

- OS reinstallation removes possible firmware modifications

Leave phones out of critical meetings or remove batteries

But when in unfamiliar territory, it is a very good idea not to leave your phone out of sight either

- If you know that you are going to a place where your phone has to be left at reception, take a tamper evident envelope or other container with you

# Is This Phone Being Spied On?

Like any other investigation, collect what you know

What made the user suspicious of spying?

- Were there extra charges on the phone bill, or new activity?
- Did someone else appear to know something that was he or she should not known?

Does the phone behave strangely?

- Did the phone open data connections out of the blue?
- If the phone is rebooted, are there any dialogs or screens that flash and suddenly disappear?

# Analyzing the Suspected Phone

- Traffic analysis
- Process analysis
- File system analysis

# Detecting Spy Tools Using Traffic Costs

A spy tool must be able to send user data out

- Practically, this means over an SMS, MMS, or Data channel
- And even if the tool is able to completely hide on the device without any indication it is there…
- No tool can escape the operator's billing system
- Of course, the user probably has an SMS/Data plan that will hide almost any traffic, if he ever even sees the phone bill
- So what you need is an investigation SIM card
- One that is not used for anything else, is as expensive as it can be and from operator that has real-time bill monitoring

# Using Basic SIM Card To Catch A Spy

Insert your investigation SIM card into the phone

- Send 20 or more SMS messages to the phone
- Make 10 phone calls to the phone
- This of course might tip off the spy, so use your imagination
- All of this should be free for the receiver
- So if there are charges in the phone bill, something bad is going on
- The same can be done with e-mail but then there will be some transfer costs for retrieving the mail to the phone

# Trying SIM Trick With E90

Remaining free data before spy activity

Liittymän saldo

| | |
|---|---|
| **Liittymä:** | |
| **Laskutuskausi:** 13.1.2008 - 22.2.2008 | |
| **Liittymäsi laskun summa ajalta 13.1.2008-20.1.2008 on noin:** | 10,19 €. |
| Kotimaan puhelut | 0,00 € |
| Ulkomaan puhelut | 0,00 € |
| Tekstiviestit | 0,40 € |
| Kuukausimaksuun sisältyvää tiedonsiirtoa jäljellä | 8,77 Mt |

After spy activity

Liittymän saldo

| | |
|---|---|
| **Liittymä:** | |
| **Laskutuskausi:** 13.1.2008 - 22.2.2008 | |
| **Liittymäsi laskun summa ajalta 13.1.2008-20.1.2008 on noin:** | 10,79 €. |
| Kotimaan puhelut | 0,00 € |
| Ulkomaan puhelut | 0,00 € |
| Tekstiviestit | 1,00 € |
| Kuukausimaksuun sisältyvää tiedonsiirtoa jäljellä | 8,75 Mt |

# Detecting Spy Tools By TCP/IP Monitoring

Some spy tools leak data over TCP/IP

- So simply watching the GPRS data icon after an SMS gives a clue
- But TCP/IP can also be sniffed, so you can actually see what is happening
- A word of warning, make sure that sniffing your own data is still legal in the country that you are operating within

Tools needed

- WLAN access point
- PC with two network ports, or good old 10BaseT hub
- Wireshark or other sniffer

# Setting Up Phone For Wireshark

## Windows Mobile

- Connect to WLAN access point
- All data should now be automatically routed over WLAN

## Symbian

- Modify all existing access points so that they use WLAN instead of packet data
- Reboot the phone and web browse a bit to open connection
- FlexiSpy insists on using GPRS, and creates own access point “ACN GPRS”; probably there are other tools that behave the same, but extra access point is a dead giveaway

# Monitoring Traffic Caused By Mobile Spy

| | | | | | |
|---|---|---|---|---|---|
| 427 | 556.694331 | 192.168.6.100 | 216.239.138.236 | HTTP | POST /webapi/sms.php HTTP/1.1 |
| 430 | 556.988250 | 192.168.6.100 | 216.239.138.236 | TCP | hpvmmdata > http [ACK] Seq=122 |
| 431 | 557.143565 | 192.168.6.100 | 216.239.138.236 | HTTP | GET /webapi/calllog.php?sID=53 |
| 435 | 557.561013 | 192.168.6.100 | 216.239.138.236 | TCP | hpvmmdata > http [ACK] Seq=132 |
| 441 | 569.228295 | 192.168.6.100 | 216.239.138.236 | TCP | ardus-cntl > http [RST] Seq=1 |
| 443 | 572.558710 | 192.168.6.100 | 216.239.138.236 | TCP | hpvmmdata > http [ACK] Seq=132 |

```
⊞ Frame 427 (1100 bytes on wire, 1100 bytes captured)
⊞ Ethernet II, Src: Cisco-Li_d8:4e:3c (00:18:f8:d8:4e:3c), Dst: Wincomm_00:6f:ee (00:01:da:00:6f:ee)
⊞ Internet Protocol, Src: 192.168.6.100 (192.168.6.100), Dst: 216.239.138.236 (216.239.138.236)
⊞ Transmission Control Protocol, Src Port: hpvmmdata (1126), Dst Port: http (80), Seq: 177, Ack: 26, Le
⊞ [Reassembled TCP Segments (1222 bytes): #424(176), #427(1046)]
⊟ Hypertext Transfer Protocol
  ⊞ POST /webapi/sms.php HTTP/1.1\r\n
    Content-Type: application/x-www-form-urlencoded\r\n
    Content-Length: 1046
    Connection: Keep-Alive\r\n
    Expect: 100-continue\r\n
    Host: www.mobile-spy.com\r\n
    \r\n
⊟ Line-based text data: application/x-www-form-urlencoded
    sID=530&content=2008-02-16\t14:29:00\t15400\t0\t2/5: KONTAKTIT(osoitemuistio), MAPPI(tekSti- ja mms
    2008-02-16\t14:29:00\t15400\t0\t5/5:ASETUKSET (wap- ja mms-asetukset sek\344 gprs-kytkent\344 nross
    2008-02-16\t14:29:00\t15400\t0\t4/5: Ohjeita palvelujen k\344ytt\366\366n saat lis\344\344m\344ll\3
    2008-02-16\t14:29:00\t15400\t0\t1/5: Soneran palvelujen hakusanat numerossa 15400 ovat: LASKU, BILL
    2008-02-16\t14:29:00\t15400\t0\t3/5: NET(www.sonera.fi/omatsivut -salasana),TEKSTI,SPOSTI(ryhm\344t
    2008-02-16\t14:33:00\t15400\t0\tPalvelu on tilap\344isesti pois k\344yt\366st\344. Yrit\344 my\366h
    2008-02-16\t14:29:33\t0\t15400\tlista\r\n
    2008-02-16\t14:33:00\t0\t15400\tmaksupaiva\r\n
```

# Process Analysis

Check every running process on the phone

- Reboot the phone and check suspected the process list against a clean phone's list
- Normally there should be very few third party tools starting right at boot
- Also on a normal phone, most processes start from the ROM image, so anything that uses a "system-ish" process name and starts from C: is interesting
- For every process that you cannot verify to be part of the OS or a clean install, check from where the image was loaded and get the sample file for closer study

# File System Analysis

So far we have not seen mobile rootkits

- If you know where to look, you can find any spy tool

Get an identical clean phone and compare with that

- Check what applications start at boot
- Get a full copy of the file system and compare against clean
- Check application install logs; any third party application without install log history is very interesting
- Install a file monitor and compare file access behavior on clean and suspected devices when receiving SMS or incoming call

# File Analysis Tools

- Memory cards that work with the phones you have
- Memory card reader
- Strings tool to get readable data from files
  - http://technet.microsoft.com/en-us/sysinternals/bb897439.aspx
- Diff to compare clean and suspected phone file dumps
  - I use Diff from Cygwin http://cygwin.com/

## Symbian S60 2nd edition

# Nokia N72 and older

- 6600, 6630, N90, N70, etc

# Analysis Tools For S60 2nd Edition

File manager and process viewer

- F-Explorer http://www.gosymbian.com/
- Efileman http://www.psiloc.com

File monitor

- EzFileMon http://www.epocsoft.com/ezfilemon.htm

Traffic monitor

- EzSniffer http://www.epocsoft.com/ezsniffer.htm

# Process Analysis On S60 2nd Edition

Processes can do whatever they wish on S60 2nd ed

- Hide from normal process list
- Assume system process name
- Fake their UID

Locating suspicious processes is a lot of work

- Fortunately most spy tools don't try to hide their processes
- And even those that do cannot fake the information from where executable was loaded

# Locating Processes On S60 2nd ed

- Start Fexplorer
- Go to processes
- Iterate every process and look for ones that do not start from Z: drive
- Normal phone has only couple user applications that are constantly running, so checking them out is worthwhile

# File Analysis On S60 2nd Edition

Drive letters

- C:\ User data and applications D:\ Temp RAM drive
- E:\ Memory card Z:\ OS ROM

Applications can be executed from anywhere

- So, well behaving ones are at c:\system\apps
- Those that don't behave well, happy hunting

Locating applications that start on boot

- Check C:\System\recogs and E:\system\recogs
- All third party applications must have .MDL file there. Typically there should be only couple well known recognizers; treat anything you don't know with suspicion

# Investigating Suspicious Files

- Scan the files with AV
- Get strings output
  - MDL files usually only load some main application, so check do you see the application name in strings
  - Strings data also contains list of libraries loaded by application
  - Anything that refers to SMS, MMS or TCP/IP communication is interesting.
  - HTTP.DLL,GSMU.DLL,MSGS.DLL,etc

# Symbian S60 3rd edition

## N73 and newer

- N73,E60,E90, etc

# Analysis Tools On Symbian S60 3rd Edition

File managers

- F-Explorer Beta http://www.gosymbian.com
- You need to get devcert on the phone in order to use it
- Y-Browser http://www.drjukka.com/YBrowser.html
- Does not show everything, but doesn't require dev cert

Process viewers

- Y-Tasks http://www.drjukka.com/YTasks.html
- Good collection of tools for getting information on running processes

# Process Analysis On S60 3rd Edition

Use Y-tasks to browse through process info

- Check all apps that are hidden or launched in background
- Check all running tasks, check whether they are hidden and what capabilities they have
  - Anything that has NetworkServices, PowerMgmt, location or other not so common capability is interesting

If still nothing, check all processes

- Focus especially on those that start from C:\ are third party and have interesting capabilities

# Symbian Security Model On S60 3rd

The Symbian security model makes our life difficult

- Normal applications cannot see executable install dir
- So a file manager that runs with normal rights is of no use
- What you need is developer cert that has “all files” capability
- Dev certs have to be requested individually for each phone
  - www.symbiansigned.com
- The good news is that applications are also limited on where they are located and how they can hide in the system

# Symbian Security Restrictions On Applications

Applications must be installed from SIS files

- Any application with significant access must be signed
- Thus for every interesting application you know who made it and what capabilities it has

Applications must be installed to proper path

- Executables must be in C:\sys\bin\
- Private data c:\private\APPUID\
- Resource data c:\resource\apps
- So applications cannot hide in location X

# File Analysis On S60 3rd Edition

## Check auto start programs

- Get all files from c:\PRIVATE\101f875a\startup\
- The .dat files contain links to programs starting on boot

## Get list of installed applications

- Get all files from c:\sys\install\sisregistry
- Each installed application has it's own subdirectory
- .ctl file contains vendor name, .reg file contains file list
- Anything that is not installed to Z: drive or by Nokia and is not visible in application manager is very interesting

# File Analysis On S60 3rd Edition

Check all executables

- C:\sys\bin if it executes, it has to be here
- Look for any application that is not present on clean phone
- For interesting applications
  - Check Application UID, litte endian DWord at 0x08-0xC
  - Check applications private data, f.ex C:\PRIVATE\2000B2C2
  - Check C:\system\apps\, f.ex C:\system\apps\2000B2C2

# Investigating Suspicious Files on S60 3rd edition

- Investigating files on S60 3rd edition is almost the same as S60 2nd edition, except that almost all executables are packed
- So you need to unpack the files before you can get strings data for them
  - Use elftran from Symbian SDK
  - “Elftran –nocompress file.app”
  - Also check out “elftran –dump s file.app”

# Windows Mobile

HTC tytn, HTC tytn II, etc

# Analysis Tools on Windows Mobile

File managers

- Resco Explorer http://www.resco.net/
- Total Commander http://www.ghisler.com/ce.htm

Registry editors

- Resco registry editor http://www.resco.net/

Process monitors

- acbTaskMan http://www.acbpocketsoft.com

# Process Analysis On Windows Mobile

Use process monitor and check all running files

- Windows mobile is very much like Windows
- Which means that even plain vanilla installation has a lot of third party applications
- Fortunately most Windows Mobile processes are well known, and Google as information on them

# File Analysis on Windows Mobile

Check application install data

- HKEY_LOCAL_MACHINE\security\AppInstall

Check auto start information

- C:\windows\startup
- HKEY_LOCAL_MACHINE\init
- HKEY_LOCAL_MACHINE\services

Check the whole file system

- Comparing against clean dump is about the only way to find something if autostart info does not give any clue

# Ok, So You Found Something Interesting

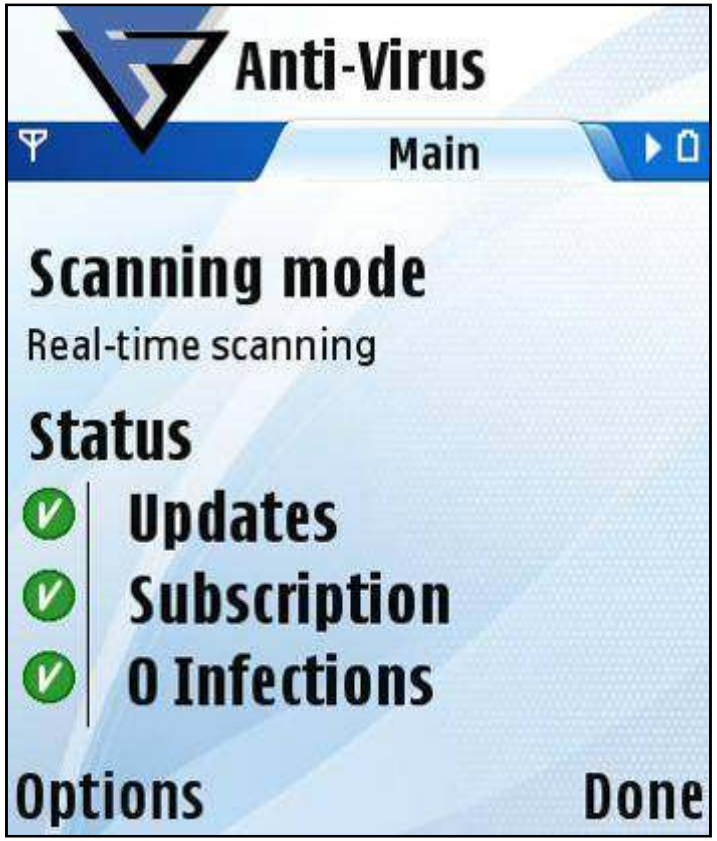
The next step is to analyze and identify the file

- Double check that the file you found is indeed the culprit
- Kill the suspicious process, and see if the spying continues
- The spy tool most likely uses some kind of resource file to contain user ID for server, or SMS number where to leak info
- In case it is a known spy tool, someone else might have already analyzed it. Google using file names or other info

And of course your friendly AV company appreciates any samples of interesting cases you find

- http://www.f-secure.com/samples/

# F-Secure Mobile Anti-Virus (+ Firewall)


F-SECURE®
BE SURE.

# F-Secure Mobile Anti-Virus


## Runs on lots of platforms

### F-Secure Mobile Anti-Virus™

- S60 2nd and 3rd edition (Symbian 7.x, 8.x and 9.x)
- Windows Mobile 2003 for Pocket PC 2003 SE/Phone edition
- Windows Mobile 2003 for Smartphone 2003 SE
- Windows Mobile 5.0 for Pocket PC
- Windows Mobile 5.0 for Smartphone


### F-Secure Mobile Security™

- Series 80 (Nokia Communicators 9300, 9300i, 9500)
- S60 3rd edition (Symbian 9.x)

F-SECURE®
BE SURE.

# BE SURE.